McAfee ePolicy Orchestrator 4.5 Installation Guide

McAfee®

COPYRIGHT

Copyright © 2009 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

License Attributions

Refer to the product Release Notes.

Contents

Pre-Installation **5**

System requirements 5

Server and Agent Handler requirements 5

Database requirements 7

Database considerations 8

Distributed repositories 10

Supported products and components 10

Operating systems language support 11

First-Time Installation **13**

Installing the server 13

Installing an Agent Handler 15

Upgrading to ePolicy Orchestrator 4.5 . . . . . **17**

Removing unused consoles 17

Unsupported products 17

Performing backups before upgrading 18

Upgrading the ePO server from version 3.6.1 18

Upgrading the ePO server from version 4.0 20

Post-Installation Tasks **22**

Completing a first-time installation 22

Completing an upgrade 22

Migrating events from version 3.6.1 23

Files to check in manually 23

Configuring the software for a server with multiple NICs 24

Uninstalling the software 24

Troubleshooting **26**

Common installation messages and their solutions 26

Default locations of troubleshooting log files 29

Installing in a Cluster Environment **31**

Windows server 2003 31

Requirements 31

Setting up the ePolicy Orchestrator cluster. 32
Testing the ePolicy Orchestrator cluster. 34
Uninstalling ePolicy Orchestrator 35
Windows server 2008. 35
Requirements. 35
Setting up the ePolicy Orchestrator cluster 36
Testing the ePolicy Orchestrator cluster. 39
Uninstalling ePolicy Orchestrator. 39

Pre-Installation

Before installing ePolicy Orchestrator 4.5, review these requirements and recommendations.

Contents

- System requirements
- Supported products and components
- Operating systems language support

System requirements

Verify that your environment meets the minimum requirements listed here:

- Server and Agent Handler
- Database
- Distributed repositories

Server and Agent Handler requirements

Free disk space — 1 GB minimum (first-time installation); 1.5 GB minimum (upgrade); 2 GB recommended.

Memory — 1 GB available RAM; 2–4 GB recommended.

Processor — Intel Pentium III-class or higher; 1 GHz or higher.

Monitor — 1024x768, 256-color, VGA monitor.

NIC — Network interface card; 100 MB or higher.

NOTE: If using a server with more than one IP address, ePolicy Orchestrator uses the first identified IP address. If you want to use additional IP addresses for agent-server communication, see *Installing an Agent Handler*.

Dedicated server — If managing more than 250 computers, McAfee recommends using a dedicated server.

File system — NTFS (NT file system) partition recommended.

IP address — McAfee recommends using static IP addresses for ePO servers.

Server-class operating system — 32bit or 64bit

- Windows Server 2003 Enterprise with Service Pack 2 or later
- Windows Server 2003 Standard with Service Pack 2 or later
- Windows Server 2003 Web with Service Pack 2 or later
- Windows Server 2003 R2 Enterprise with Service Pack 2 or later

- Windows Server 2003 R2 Standard with Service Pack 2 or later
- Windows Server 2008

  NOTE: Installation is blocked if you attempt to install on a version of Windows earlier than Server 2003. In addition, ePolicy Orchestrator stops functioning if, after having been installed on Windows Server 2003, the server is upgraded to Windows Server 2008.

Browser

- Firefox 3.0
- Microsoft Internet Explorer 7.0 or 8.0

  If using Internet Explorer and a proxy, follow these steps to bypass the proxy server.

  1 From the **Tools** menu in Internet Explorer, select **Internet Options**.
  2 Select the **Connections** tab and click **LAN Settings**.
  3 Select **Use a proxy server for your LAN**, then select **Bypass proxy server** for local addresses.
  4 Click **OK** as needed to close Internet Options.

Domain controllers — The server must have a trust relationship with the Primary Domain Controller (PDC) on the network. For instructions, see the Microsoft product documentation.

Security software

- Install and/or update the anti-virus software on the ePolicy Orchestrator server and scan for viruses.

  CAUTION: If running VirusScan Enterprise 8.5i or 8.7i on the system where you are installing ePolicy Orchestrator, you must ensure that the VSE Access Protection rules are disabled during the installation process, or the installation fails.

- Install and/or update firewall software on the ePolicy Orchestrator server.

Ports

- McAfee recommends avoiding the use of Port 8443 for HTTPS communication. Although this is the default port, it is also the primary port used by many web-based activities, is a popular target for malicious exploitation, and it is likely to be disabled by the system administrator in response to a security violation or outbreak.

  NOTE: Ensure that the ports you choose are not already in use on the ePolicy Orchestrator server computer.

- Notify the network staff of the ports you intend to use for HTTP and HTTPS communication via ePolicy Orchestrator.

  NOTE: Installing the software on a Primary Domain Controller (PDC) is supported, but not recommended.

Supported virtual infrastructure software

- VMware ESX 3.5.x
- Microsoft Virtual Server 2005 R2 with Service Pack 1
- Windows Server 2008 Hyper-V

Database requirements

Microsoft updates and patches

Update both the ePO server and the database server with the latest Microsoft security updates. If you are upgrading from MSDE 2000 or SQL 2000, be sure to follow Microsoft's required upgrade scenarios.

Databases supported for use with ePolicy Orchestrator

- SQL Server 2005 Express. This database is included with ePolicy Orchestrator for use in environments where there is no supported database available.
- SQL Server 2005.
- SQL Server 2008 Express.
- SQL Server 2008.

NOTE: Use of ePolicy Orchestrator with MSDE 2000 or SQL 2000 (or earlier) is not supported.

Database installation documented in this Guide

The only database installation scenario described in detail is a first-time installation of SQL Server 2005 Express. In this scenario, the ePOSetup installs both the ePolicy Orchestrator software and the database on the same server. If the database is to be installed on a different server from the ePolicy Orchestrator software, manual installation is required on the remote servers.

Other relevant database installations and upgrades

See the documentation provided by the database manufacturer for information about the following installation scenarios:

- Installing SQL Server 2005.
- Installing SQL Server 2008.
- Upgrading from MSDE 2000.
- Upgrading from SQL 2000.
- Upgrading from SQL 2005.
- Upgrading from SQL 2005 Express.
- **Maintenance settings** — McAfee recommends making specific maintenance settings to ePO databases. For instructions, see *Maintaining ePO databases* in the *ePolicy Orchestrator Help.*

SQL Server

- **Dedicated server and network connection** — Use a dedicated server and network connection if managing more than 5,000 client computers.
- **Local database server** — If using SQL Server on the same system as the ePOserver, McAfee recommends using a fixed memory size in Enterprise Manager that is approximately two-thirds of the total memory for SQL Server. For example, if the computer has 1GB of RAM set 660MB as the fixed memory size for SQL Server.

- **SQL Server licenses** — If using SQL Server, a SQL Server license is required for each processor on the computer where SQL Server is installed.

  CAUTION: If the minimum number of SQL Server licenses is not available after you install the SQL Server software, you may have issues installing or starting the ePolicy Orchestrator software.

Database considerations

Using ePolicy Orchestrator with a database

A database must be installed before ePolicy Orchestrator can be installed. Any of the following databases, if previously installed, meets this requirement.

- SQL Server 2005
- SQL 2005 Express
- SQL 2008
- SQL 2008 Express

  NOTE: SQL 2000 is not supported.

If none of those databases was previously installed, the ePO installation wizard detects that no database is present and offers you the opportunity to install SQL Server 2005 Express.

The following tables provide additional information about the database choices and other software requirements.

Database	Requirements	Note
SQL Server 2005 or SQL Server 2008	Dedicated server and network connection	Needed if managing more than 5,000 computers.
	Local database server	If the database and ePO server are on the same system, McAfee recommends using a fixed memory size in Enterprise Manager or SQL Server Management Studio that is approximately two-thirds of the total memory for SQL Server. For example, if the computer has 1 GB of RAM, set 660 MB as the fixed memory size for SQL Server.
	Licenses	A license is required for each processor on the computer where SQL Server is installed. If the minimum number of SQL Server licenses is not available, you might have difficulty installing or starting the ePolicy Orchestrator software.
SQL Server 2005 Express	.NET Framework	You must acquire and install.

Software	Note
MSXML 6.0	You must acquire and install. 1 From the Internet Explorer **Tools** menu, select **Windows Update**. 2 Click **Custom**, then select **Software**. 3 Select **MSXML6**. 4 Select **Review and install updates**, then click **Install Updates**.

Software	Note
Internet Explorer 7 or 8, or Firefox 3.0	You must acquire and install.
.NET Framework 2.0	You must acquire and install if using SQL Server 2005 Express.
Microsoft Visual C++ Redistributable	If not previously installed, the installation wizard installs automatically.
Microsoft Visual C++ Redistributable - x86 9.0.21022	If not previously installed, the installation wizard installs automatically.
MDAC 2.8	If not previously installed, the installation wizard installs automatically.
SQL Server 2005 Backward Compatibility	If not previously installed, the installation wizard installs automatically.
SQL Server 2005 Express	If no other database has been previously installed, this database can be installed automatically at user's selection.
Microsoft updates	Update the ePolicy Orchestrator server and the database server with the most current updates and patches.
MSI 3.1	The installation fails if using a version of MSI previous to MSI 3.1.

Database installation documented in this guide

The only database installation scenario described in detail is a first-time installation of SQL Server 2005 Express. In this scenario, the ePolicy Orchestrator Setup installs both the ePolicy Orchestrator software and the database on the same server. If the database is to be installed on a different server from the ePolicy Orchestrator software, manual installation of SQL is required on the remote server.

Other relevant database installations and upgrades

See the documentation provided by the database manufacturer for information about the following installation scenarios:

- Installing SQL Server 2005 or 2008.
- Upgrading from MSDE 2000 to SQL Server 2005 or 2008.
- Upgrading from MSDE 2000 to SQL Server 2005 Express.

Nested triggers — The SQL Server Nested Triggers option must be enabled.

Database collation — The only database collation supported by ePolicy Orchestrator is the U.S. English default: SQL_Latin1_General_Cp1_CI_AS.

Maintenance settings — McAfee recommends making specific maintenance settings to ePolicy Orchestrator databases. For instructions, see *Maintaining ePolicy Orchestrator databases* in the ePolicy Orchestrator 4.5 Help.

SQL Server

Dedicated server and network connection — Use a dedicated server and network connection if managing more than 5,000 client computers.

Local database server — If using SQL Server on the same system as the ePolicy Orchestrator server, McAfee recommends using a fixed memory size in Enterprise Manager that is approximately two-thirds of the total memory for SQL Server. For example, if the computer has 1 GB of RAM, set 660 MB as the fixed memory size for SQL Server.

SQL Server licenses — If using SQL Server, a SQL Server license is required for each processor on the computer where SQL Server is installed.

CAUTION: If the minimum number of SQL Server licenses is not available after you install the SQL Server software, you might have issues installing or starting the ePolicy Orchestrator software.

Distributed repositories

Free disk space — 400 MB on the drive where the repository is stored.

NOTE: The disk space requirement for the distributed repositories on agents that are designated as SuperAgents is equal to the disk space available for the master repository.

Memory — 256 MB minimum.

Possible hosts:

- HTTP-compliant servers on Microsoft Windows, Linux, or Novell NetWare operating systems
- Windows, Linux, or NetWare FTP servers
- Windows, Linux, or UNIX Samba UNC shares
- Computer with a SuperAgent installed on it

Supported products and components

- McAfee Agent 4.0 for Email and Web Security
- McAfee Agent 4.0 for HP-UX
- McAfee Agent 4.0 for Linux
- McAfee Agent 4.0 for Macintosh
- McAfee Agent 4.0 for Solaris
- McAfee Agent 4.5
- McAfee Agent for Windows Patch 1 and Patch 2
- McAfee Common Management Agent 3.7 Patch 1
- McAfee Common Management Agent MA 3.6 Patch 4
- McAfee Data Loss Prevention 2.1 Patch 2
- McAfee Data Loss Prevention 2.2
- McAfee Data Loss Prevention 3.0
- McAfee Email and Web Security 5.1 Appliance
- McAfee Endpoint Encryption 5.2.1
- McAfee Endpoint Encryption 5.3
- McAfee Endpoint Encryption Files/Folders 3.1 (EEFF)
- McAfee Endpoint Encryption Files/Folders 4.x (EEFF)
- McAfee EndPoint Encryption for Mobile 3.0 (EEMO)
- McAfee Foundstone 6.5.3
- McAfee GroupShield for Domino 7.0
- McAfee GroupShield for Exchange 6.0.2 with SKE

- McAfee GroupShield for Exchange 7.0
- McAfee GroupShield for Exchange 7.0 SP 1
- McAfee Host Intrusion Prevention 6.1 Patch 3
- McAfee Host Intrusion Prevention 7.0 Patch 3
- McAfee Host Intrusion Prevention 7.1
- McAfee IntruShield 4.1
- McAfee IntruShield 5.1
- McAfee LinuxShield 1.5.1
- McAfee Network Access Control 3.1
- McAfee Policy Auditor 5.1 (Feyman)
- McAfee PortalShield 2.0 Patch 1
- McAfee Quarantine Manager 6.0
- McAfee Rogue System Detection 2.0 Patch 2
- McAfee Security for Lotus Domino Linux 7.5
- McAfee Security for Macintosh v1.0
- McAfee SiteAdvisor Enterprise 1.6
- McAfee SiteAdvisor Enterprise 2.0+
- McAfee SiteAdvisor Enterprise 3.0
- McAfee VirusScan 8.5i with McAfee AntiSpyware Enterprise
- McAfee VirusScan 8.7 with McAfee AntiSpyware Enterprise
- McAfee VirusScan Advanced Server (NetApp)
- McAfee VirusScan Advanced Server (SAP)
- McAfee VirusScan Advanced Server (Virtualization)
- McAfee VirusScan for Macintosh 8.6.1
- Symantec SAV 10.x
- Symantec SAV 9.x
- USB Device 1.0 (EEV)
- Vdisk 4.1 (EEV)
- vDisk for Macintosh 1.0

Operating systems language support

This version of the ePolicy Orchestrator software runs on any supported operating system irrespective of the language of the operating system.

Following is a list of languages into which the ePolicy Orchestrator has been translated. When the software is installed on an operating system using a language that is not on this list, the ePolicy Orchestrator interface attempts to display in English.

- Chinese (Simplified)
- Chinese (Traditional)
- English
- Japanese
- Korean
- Russian

- French (Standard)
- German (Standard)
- Spanish

First-Time Installation

This chapter provides instructions for installing ePolicy Orchestrator 4.5 in an environment where no previous version of ePolicy Orchestrator software has been installed.

CAUTION: If you are upgrading from a prior version of ePolicy Orchestrator or are migrating from an evaluation version, see *Upgrading to ePolicy Orchestrator 4.5*.

Be sure that you have read, understood, and complied with the requirements and recommendations in *Pre-Installation*.

Contents

- Installing the server
- Installing an Agent Handler

Installing the server

The installation depends, in part, upon the presence of MSXML 6.0 on the server. If it is not present, an error message appears during the installation, advising you that it must be installed before proceeding. To avoid the inconvenience of interfering with the installation in order to download and install MSXML, we strongly recommend that you obtain and install MSXML before starting the installation.

We also recommend that you monitor the entire installation process. It might require you to restart the system.

Use this task to install the ePolicy Orchestrator server.

Task

1. Using an account with local administrator permissions, log on to the Windows server computer to be used as the ePO server .
2. Run the Setup program.
   - From the product CD: select a language in the ePolicy Orchestrator autorun window, then select **Install ePolicy Orchestrator 4.5**.
   - From software downloaded from the McAfee website: go to the location containing the extracted files and double-click **Setup.exe**. The executable is located in the file **EPO 4.5.0 <build and package numbers>.zip**. Be certain to extract the contents of the zip file to a temporary location. Do not attempt to run Setup.exe without first extracting the contents of the zip file.

   NOTE: If any prerequisite software is missing from the installation target computer, a list of those items appears.
3. Click **Next**. The installation process for each software item not listed as Optional begins automatically.

If you intend to use an existing instance of SQL Server 2005, or SQL 2008, you can continue without selecting the checkbox for installation of SQL Server 2005 Express.
If you do not have a supported version of SQL or MSDE, take one of the following actions:

- Install SQL 2005 or 2008 on a server.

  If you are installing ePolicy Orchestrator with SQL 2005, the SQL Browser must be enabled or you cannot complete the installation wizard.
- Install SQL Server 2005 Express on the same computer where you are installing ePolicy Orchestrator. If you selected the checkbox for installation of SQL Server 2005 Express, ePolicy Orchestrator installs the database automatically.

  If you are installing SQL Server 2005 Express, you might be prompted to install SQL Server 2005 Backward Compatibility. You must install it.

4 In the Welcome page of the installation wizard, click **Next**. The License Key page appears.

NOTE: License Keys are distributed from the same McAfee website from which the ePolicy Orchestrator software is downloaded.

5 Select whether you are installing based on a license key or installing an evaluation version.

- If you have a License Key, type its number here.
- If you select **License Key** but do not type its number you are asked if you want to install an evaluation version. Click **OK** to proceed with installation of the evaluation version, or **Cancel** to return to the previous page.

6 If you are installing a beta version of the software, the Beta test information box appears. Click **OK**.

7 Accept the **End User License Agreement**, then click **OK** to continue. The Choose Destination Location dialog box appears. Click **Next**.

8 Accept the default installation path or click **Browse** to select or create a different location, then click **Next**.
If installing on a cluster server, the Set Database and Virtual Server Settings dialog box appears. Otherwise the **Set Administrator Information** dialog box appears.

9 Type and verify the password for logging on to this ePolicy Orchestrator server, then click **Next**.
If your environment employs Microsoft Cluster Server (MSCS) for a high availability system that ensures failover support, the Set Database and Virtual Server Settings dialog box appears.

10 In the Set Database Information dialog box, identify the type of account and authentication details that the ePO server will use to access the database:

a Use the drop-down list to select a database server. If SQL Express was installed, the name of the database is **<computername>\EPOSERVER**.

b Select the type of authentication, then click **Next**.

- **Windows authentication** *(recommended)* — Specify the NetBIOS name of the **Domain** associated with the desired domain administrator user account. Then, provide and verify a password.

  NOTE: If the database identification fails, type 1433 or 1434 in the **SQL server TCP port** field.

- **SQL authentication** — Provide the **User name** that the ePolicy Orchestrator software will use to access the database, then provide a password. If the installer cannot identify

the port used for communication to and from the server, you might be prompted to provide that information.

NOTE: The ePolicy Orchestrator account must have DB ownership to the database.

11 Set the **HTTP Configuration**. Designate the port to be used by each function, then click **Next**.

Function	Port
Agent-to-Server communication port	Configurable. McAfee recommends using a port other than 80.
Agent Wake-Up communication port	Configurable.
Agent Broadcast communication port	Configurable port used to send SuperAgent wake-up calls.
Console-to-Application Server communication port	Configurable.
Sensor-to-Server communication port	Configurable port used by the Rogue System sensor to report host-detected messages to the Rogue System Detection server using SSL.
Security Threats communication port	Port 8801. Nonconfigurable port used by McAfee Avert to provide information on security threats and the required DAT and engine versions to protect against them.
SQL server TCP port	See SQL documentation for configuration information.

NOTE: Client firewalls block communication from the ePO server. Ensure that the ports required for communication from the ePO server are available on the client.

12 *Optional step (can be performed after ePolicy Orchestrator is up-and-running).* In the Default Notification Email Address dialog box, type the email address of the recipient of messages from ePolicy Orchestrator notification or leave the default. For a new recipient, complete these options, then click **Next**.

a Provide a default destination for messages.

b Select **Setup email server settings now**. However, if you choose **Setup email server settings later**, leave the default address.

c Type the Fully Qualified Domain Name (FQDN) of the mail server and specify the **Port** to use for email.

d Select **This server requires authentication** if needed, then type the **User name** and **Password** required to access the server.

For more information, see *Automatic Responses* in the *ePolicy Orchestrator 4.5 Product Guide*.

13 In the Start Copying Files dialog box, click **Next** to begin the installation.

14 In the Installation Complete dialog box, you can view the Release Notes, launch ePolicy Orchestrator, or click **Finish** to complete the installation.

Installing an Agent Handler

Use this task to set up an Agent Handler.

Before you begin

You must first install the ePO server with which the Agent Handler is to communicate.

Task

1. Open the folder where you extracted the contents of the ePolicy Orchestrator installation package.
2. Copy the **AgentHandler** folder to the intended Agent Handler server system.
3. Double-click and run **Setup.exe**. Installation activities take place in the background. When they are completed, the InstallShield Wizard for McAfee Agent Handler opens. Click **Next**.
4. Accept the default destination or click **Browse** to change the destination, then click **Next**. The Server Information page opens.
5. Type the machine name of the ePO Server with which the Agent Handler is to communicate.
6. Type the port to be used for server-handler communication. Port 8433 is the default. McAfee recommends that you change the port designation. See the discussion of *Ports* in the *Server and Agent Handler requirements* section.
7. Type the **ePO Admin User** name and password of a user with global administrator privileges. If these credentials are to be used for the database as well, click **Next** to start the installation.

   NOTE: These credentials must be identical with those used during installation of ePolicy Orchestrator.

8. If you want to use different database credentials than those mentioned in step 7, follow these additional steps:
   a. Deselect **Use ePO Server's database credentials**, then click **Next**.
   b. Type the name of the SQL database server.
   c. Select **Windows Authentication** or **SQL Authentication**, then type the credentials.

   NOTE: These credentials must be identical with those of a previously defined SQL Server user.

9. Click **Next**. The installation process begins.

Upgrading to ePolicy Orchestrator 4.5

This chapter provides instructions for upgrading an existing version of ePolicy Orchestrator to version 4.5 of the software.

Contents

- Unsupported products
- Performing backups before upgrading
- Upgrading the ePO server from version 3.6.1
- Upgrading the ePO server from version 4.0

Removing unused consoles

ePolicy Orchestrator 3.6.1 and earlier provided the option of installing remote consoles (MMC). If remote consoles are present, use Windows Add/Remove programs feature to remove them.

Unsupported products

The following products are no longer supported in version 4.5 and are not migrated.

- McAfee ePolicy Orchestrator Agent for Macintosh OS X
- McAfee ePolicy Orchestrator Agent for Linux
- McAfee ePolicy Orchestrator Agent for Netware
- McAfee NetShield 4.6.3 for NetWare
- McAfee Common Management Agent 3.5.5
- McAfee LinuxShield 1.3
- McAfee LinuxShield 1.4
- McAfee LinuxShield 1.5
- McAfee Site Advisor Enterprise 1.5
- McAfee Non-Windows Agents v2.0
- McAfee VirusScan Mobile Enterprise
- McAfee System Compliance Profiler 2.0
- McAfee Network Access Control 3.0 Patch 2
- McAfee Policy Auditor 5.0
- McAfee Policy Auditor 5.0.1
- McAfee Group Shield for Exchange 6.0

- McAfee Groups Shield for Exchange 6.0.2 with SKE RTW Repost_5200
- McAfee Virex 7.7
- McAfee VirusScan 8.0i with McAfee AntiSpyware Enterprise Patch 16
- McAfee VirusScan For Macintosh 8.5
- McAfee VirusScan For Macintosh 8.6

Performing backups before upgrading

Before you upgrade to version 4.5, back up all ePolicy Orchestrator databases, as well as the ePO directory. Additional information is available in the following Knowledge Base articles:

ePolicy Orchestrator Version	KB article
3.6x	KB53219
4.0	KB51438

Upgrading the ePO server from version 3.6.1

This task upgrades the ePO server from ePolicy Orchestrator version 3.6.1 Patch 4 or later to version 4.5. McAfee recommends that you monitor the upgrade process. It might require you to restart the system.

The default location of version 3.6.1 is:

C:\Program Files\McAfee\ePO\3.6.1

Before you begin

You must install the SQL 2005 Backwards Compatibility package before upgrading an ePolicy Orchestrator installation if you are using a remote database server or a local SQL 2005 server that does not already have it installed.

Task

1. Log on to the desired system using an account with local administrator permissions.
2. If you are using Microsoft SQL Server 2005 or 2008, verify that it is running.
3. Run the Setup program.
   - From the product CD: select a language in the ePolicy Orchestrator autorun window, then select **Install ePolicy Orchestrator 4.5**.
   - From software downloaded from the McAfee website: go to the location containing the extracted files and double-click **Setup.exe**.

     NOTE: If any prerequisite software is missing from the installation target computer, a list of those items appears. Click **Next**. The installation process for each software item not listed as Optional begins automatically. For Optional items, a dialog box appears, where you can allow installation or reject it.
4. In the Welcome window of the installation wizard, click **Next**. A warning message lists which products are no longer supported with this version of the software. These products are not migrated to the ePolicy Orchestrator 4.5 Repository.

5 In the Choose Destination Location dialog box, accept the default installation path or click **Browse** to select a different location, then click **Next**.
If installing on a cluster server, the Set Database and Virtual Server Settings dialog box appears. Otherwise the **Set Administrator** Information dialog box appears.

6 In the **Set Administrator Information** dialog box, type and verify the user name and password for logging on to this ePO server for the first time, then click **Next**. For security reasons, ePolicy Orchestrator does not allow accounts with blank passwords.

7 In the Set Database Information dialog box, identify the type of account and authentication details that the ePO server will use to access the database.
Indicate whether ePolicy Orchestrator will use a Windows NT user account or a SQL Server user account. McAfee recommends using Windows NT authentication.

NOTE: The name of the database server that was set during the original installation cannot be changed here.

- **Windows authentication** *(recommended)* — Specify the NetBIOS name of the **Domain** associated with the desired domain administrator user account. Then, provide and verify a password.
- **SQL authentication** — Provide the **User name** that ePolicy Orchestrator will use to access the database, then provide a password. If the installer cannot identify the port used for communication to and from the server, you might be prompted to provide that information. Otherwise, the SQL server TCP port field shows the port and is disabled.

  When upgrading an installation using NT authentication, the Set Database Information panel of the wizard appends the domain name to the User name field and auto-populates the port field with 1433. Remove the domain from the User name field and click **Next**. You will receive a port error. Dismiss this error and manually retype the port number 1433, then click **Next**.
- For security reasons, ePolicy Orchestrator does not accept accounts with blank passwords.

NOTE: If you are installing on a system with a local SQL 2005 database server, you must manually type the TCP port number on the Set Database Information page of the installation wizard.

8 Click **Next** to display the HTTP Configuration dialog box. The values that were set during the original installation cannot be changed here.

Function	Port
Agent-to-Server communication port	Configurable. McAfee recommends using a port other than 80.
Agent Wake-Up communication port	Configurable.
Agent Broadcast communication port	Configurable port used to send SuperAgent wake-up calls.
Console-to-Application Server communication port	Configurable.
Sensor-to-Server communication port	Configurable port used by the Rogue System Sensor to report host-detected messages to the Rogue System Detection server using SSL.
Security Threats communication port	Port 8801. Nonconfigurable port used by McAfee Avert to provide information on security threats and the required DAT and engine versions to protect against them

Function	Port
SQL server TCP port	Port 1433. Nonconfigurable unless connection has failed. It then becomes configurable. See SQL documentation for additional information about configuring this port.

9 Click **Next**. In the Default Notification Email Address dialog box, type the email address for the recipient of messages from ePolicy Orchestrator Notifications, or leave the default. For a new recipient, complete these options, then click **Next**.

   a Provide a default destination for messages.

   b Select **Setup email server settings now**. If you choose **Setup email server settings later**, leave the default address.

   c Type the Fully Qualified Domain Name (FQDN) of the mail server and specify the **Port** to use for email.

   d Select **This server requires authentication** if needed, then type the **User name** and **Password** required to access the server.

   For more information, see *Automatic Responses* in the *ePolicy Orchestrator 4.5 Product Guide*.

10 In the Start Copying Files dialog box, click **Install**.

11 In the Installation Complete dialog box, click **Finish** to complete the installation.

Upgrading the ePO server from version 4.0

This task upgrades the ePO server from ePolicy Orchestrator version 4.0 Patch 3 or later to version 4.5. McAfee recommends that you monitor the upgrade process. It might require you to restart the system.

The default location of ePolicy Orchestrator version 4.0 is:

C:\Program Files\McAfee\ePolicy Orchestrator

Before you begin

You must install the SQL 2005 Backwards Compatibility package before upgrading an ePolicy Orchestrator installation if you are using a remote database server or a local SQL 2005 server that does not already have it installed.

Task

1 Log on to the desired system using an account with local administrator permissions.

2 If you are using Microsoft SQL Server 2005 or 2008, verify that it is running.

3 Run the Setup program.

- From the product CD: select a language in the ePolicy Orchestrator autorun window, then select **Install ePolicy Orchestrator 4.5**.
- From software downloaded from the McAfee website: go to the location containing the extracted files and double-click **Setup.exe**.

  NOTE: If any prerequisite software is missing from the installation target computer, a list of those items appears. Click **Next**. The installation process for each software item not listed as Optional begins automatically. For Optional items, a dialog box appears, where you can allow installation or reject it.

4 In the Welcome window of the installation wizard, click **Next**. A warning message lists which products are no longer supported with this version of the software. These products are not migrated to the ePolicy Orchestrator 4.5 Repository.

5 In the **Set Administrator Information** dialog box, type and verify the user name and password of the global administrator for the current ePO server, then click **Next**. For security reasons, ePolicy Orchestrator does not allow accounts with blank passwords.

6 In the Start Copying Files dialog box, click **Next** to begin the installation.

7 In the Installation Complete dialog box, click **Finish** to complete the installation.

Post-Installation Tasks

After completing the Setup wizard, follow the appropriate procedures to configure the software.

Contents

- Completing a first-time installation
- Completing an upgrade
- Migrating events from version 3.6.1
- Files to check in manually
- Configuring the software for a server with multiple NICs
- Uninstalling the software

Completing a first-time installation

The tasks needed to complete a first-time installation are listed here. For details about performing these tasks, see the *ePolicy Orchestrator 4.5 Product Guide*.

Tasks

1. Plan your ePolicy Orchestrator System Tree and updating scheme.
2. Create the ePolicy Orchestrator System Tree.
3. Distribute the McAfee Agent to the systems you want to manage with ePolicy Orchestrator.
4. Create the updating repositories.
5. Check in to the repositories the products ePolicy Orchestrator is to manage. Then configure their policy settings.
6. Deploy products to the managed computers.
7. Configure the advanced features of ePolicy Orchestrator.

Completing an upgrade

Perform the following tasks to complete an upgrade.

Tasks

1. Migrate events from the previous version of ePolicy Orchestrator. See *Migrating events from version 3.6.1* in this guide.
2. Plan and implement any changes you want to make to the ePolicy Orchestrator System Tree (formerly Directory) and Repository.

3 Check in and deploy new products you want to manage.

For details, see the *ePolicy Orchestrator 4.5 Product Guide.*

Migrating events from version 3.6.1

Use this task to migrate events recorded in version 3.6.1 of ePolicy Orchestrator to version 4.5. It is not necessary to migrate events from version 4.0 to version 4.5.

Task

1 Click **Menu | Automation | Server Tasks**.

2 Select the **Edit** link in the **Actions** column for the row labeled **Event Migration (3.6x->4.x)**.

3 On the Description tab, type a name for the task and any notes you want; select **Enabled**, then click **Next**.

4 On the Actions tab, ensure that **Event Migration** is selected from the drop-down Actions list. From the list of DTS (Data Transformation Services) packages, select the packages that you want to migrate.

5 To run the migration immediately, click **Finish**, then click **Run** in the Actions field.

6 To schedule the migration to run at a future time, click **Next**.
To implement the continuous migrating of events until conclusion, make the following settings on the Schedule page:

   a Select **Daily**.

   b Specify a **Start date** and make the **End date** the same.

   c Select a time of day.

   d Click **Next**.

Files to check in manually

These are the files that you must check in to the master repository after you install or upgrade the software. For more information, see the *ePolicy Orchestrator 4.5 Product Guide*.

- **Custom packages** — Only managed product packages that were created with McAfee Installation Designer 8.0 or later can be checked in to the master repository.
- **Product extensions**— If the extension for a managed product was not added to the repository during the installation, you must manually add it as a zip file.
- **Product plug-in files** — Any product plug-in (.dll) files that were not checked in as part of the installation must be checked in to the master repository manually as zip files.
- **Products** — Check the software you intend to deploy into the repository.
  - If you are installing ePolicy Orchestrator for the first time, you must check in all products that you want to deploy via ePolicy Orchestrator.
  - If you are upgrading ePolicy Orchestrator, any supported products that were not already present must be checked in to the master repository manually as zip files.
- **Product updates** — You must check in all product updates that you want to deploy via ePolicy Orchestrator.

Configuring the software for a server with multiple NICs

When you install ePolicy Orchestrator on a server with multiple network interface cards (NICs), ensure that ePolicy Orchestrator is bound to the appropriate NIC. There are three approaches to achieving this, depending on the number of IP addresses you want to expose for agent-server communication.

Task

1 Open the **server.ini** file. The default location is:
C:\Program Files\McAfee\ePolicy Orchestrator\DB

2 Modify the [server] section of the file by adding the following line:
Server=<IP address of the server you want ePolicy Orchestrator to use>

Follow the procedure that corresponds to the number of IP address you want to expose:

a **To expose a single IP address**: modify the server.ini file, and insert the IP address you want to expose.

b **To expose all IP addresses**: modify the server.ini file, and insert the FQDN of the ePO server.

c **To expose some IP addresses**: modify the server.ini file, and insert an IP address you want to expose. Then, set up a new virtual Agent Handler group to define additional IP addresses you want to expose for agent-server communication. See the *ePolicy Orchestrator Product Guide* for additional information.

NOTE: The server IP addresses are used for agent access to the master repository and for agent-server communication. If these addresses are not provided, the IP address of the first listed NIC is used.

3 Save and close the server.ini file.

4 Restart all ePO services.

Uninstalling the software

If you need to uninstall ePolicy Orchestrator software, use this procedure. If you used the ePO Setup program to install SQL 2005 Express, you can remove the database when you remove ePolicy Orchestrator.

Before you begin

You must uninstall any Agent Handlers registered to this ePO server before you uninstall the ePolicy Orchestrator.

Task

1 Close all database management software.

2 Open the **Control Panel** and select **Add/Remove Programs**.

3 Select **McAfee ePolicy Orchestrator**, then click **Remove**. The Remove McAfee ePolicy Orchestrator dialog box appears.

4 Select **Also remove the ePolicy Orchestrator database**.

5 Click **Remove**.

Troubleshooting

Use this information to troubleshoot any problems with your installation of ePolicy Orchestrator. The most common messages that appear during an installation and their solutions are listed here.

If you are unable to resolve an issue using the information in this table, contact McAfee Technical Support after you have taken the steps described below:

- Verify that you have met the minimum installation requirements.
- Review the *ePolicy Orchestrator 4.5 Release Notes* (Readme.html) for any known installation issues.
- Verify that the account you used to log on to the computer where you are installing the software has full administrator permissions to that computer.
- Collect the exact text of all messages, and be sure to write down any message codes that appear.
- Gather the installation log files.

Contents

- Common installation messages and their solutions
- Default locations of troubleshooting log files

Common installation messages and their solutions

If this message appears...	Then...
You are attempting to upgrade from a product version that is not supported. For a complete list of upgrade requirements, see the ePolicy Orchestrator Installation Guide.	No version of ePolicy Orchestrator has been installed on this computer. You can only upgrade from ePolicy Orchestrator 3.6.1 Patch 4 or later and ePolicy Orchestrator 4.0 Patch 3 or later.
Internet Explorer 7 or later, or Firefox 3.0 needs to be installed for this installation to continue.	The computer where you are attempting to install the software is using a non-supported version of the browser. Install Internet Explorer 7.0 or later, or Firefox 3.0 before you install the ePolicy Orchestrator software.
Another instance of the McAfee ePolicy Orchestrator installer is already running.	The ePolicy Orchestrator 4.5 Setup program is already running. You cannot run more than one instance of Setup at a time.
For security reasons McAfee does not allow blank passwords. Please enter a valid password to continue.	The **Password** box is blank. Specify the password of the user account that you want to use.
McAfee recommends that you set the video display to 1024x768 or higher resolution.	The computer where you are attempting to install the software does not meet the minimum monitor resolution requirement. Change the monitor resolution to 1024x768 or higher, then continue the installation. Otherwise, you might not be able to view the entire application window after you start the software. For instructions on changing

If this message appears...	Then...
	the monitor resolution, see the Windows Help File (click **Start**, then select **Help**).
McAfee recommends that you install the software on a computer with at least 1 GB of RAM.	The computer where you are attempting to install the software does not meet the minimum memory requirement.
McAfee ePolicy Orchestrator 4.5 requires that your computer is running Windows Server 2003, or Windows Server 2008.	The computer where you are attempting to install the software is using a non-supported version of the operating system.
Enter a value in the "Agent Broadcast communication" field.	The **Agent Broadcast communication port** box is blank. Specify the port number (default is 8082) that the ePolicy Orchestrator server will use to send agent wake-up calls to SuperAgents.
Enter a value in the "Agent-to-Server communication" field.	The **Agent-to-Server communication port** box is blank. Specify the port number that the agent will use to communicate with the server.
Enter a value in the "Agent Wake-Up communication" port.	The **Agent Wake-Up communication port** box is blank. Specify the port number (default is 8081) that the ePolicy Orchestrator server will use to send agent wake-up calls.
McAfee ePolicy Orchestrator must be installed in a folder. Enter a Destination Folder to continue.	The **Destination Folder** box is blank or shows the root of a drive. Click **Browse** to select a location. The default location is: C\Program Files\McAfee\ePolicyOrchestrator.
Enter a value in the "User Name" field.	The **User name** box is blank. Specify the user name of the account that you want to use.
The License file is missing is missing or corrupt. Contact support for assistance.	Setup is unable to read the license information required to install the software. Contact McAfee Technical Support.
The operating system or service pack you are using is not currently supported. For a complete list of system requirements, see the ePolicy Orchestrator Installation Guide.	The computer where you are attempting to install the software is using a non-supported version of the operating system.
The passwords you entered do not match. Enter a valid password to continue.	The value you typed in **Password** and **Confirm Password** do not match. Specify the password of the account that you want to use.
The McAfee ePolicy Orchestrator license has expired.	Your license to use the software has expired. Go to the beta feedback page on the McAfee website, where you can supply your comments about the beta software.
This system is not currently configured with a static IP address, which is recommended for the ePolicy Orchestrator server.	The computer where you are attempting to install the software does not use a static IP address. McAfee recommends using static IP addresses for ePO servers to improve performance and reduce bandwidth usage.
Unable to make a connection to the database server. Verify that you provided the account credentials and database server name correctly, then try again. If this message continues to appear, see the ePolicy Orchestrator Installation Guide for more information.	A connection could not be made to the corresponding ePolicy Orchestrator database server. **1** Verify that the **Domain**, **User Name**, and **Password** you provided are typed correctly. **2** Verify that the database server is running. **3** Verify that the user account you provided is valid for the database server.
Unable to connect using the information you provided. Verify that you entered the correct information and try again.	The user account that you specified could not be accessed. **1** Verify that the **Domain**, **User Name**, and **Password** you provided are typed correctly.

If this message appears...	Then...
	2 Verify that the account you used to log on to this computer has access to this domain.

Default locations of troubleshooting log files

Log File Name	Log Type	File Location	Description
AHSetupDLL.log	Temporary	%temp% on the Agent Handler server	Logs Agent Handler backend events
EPO450-Install-MSI.LOG	Install	%temp%\mfelogs	Main log file for the ePolicy Orchestrator 4.5.0 installer.
[ExtensionFileName].cmd	Temporary	%temp%\MFElogs\ePO4 50-troubleshoot\ OutputFiles	File created by ePolicy Orchestrator installer, containing the command (sent to Remote-Client) to check in extensions.
dbmExecute.log	Temporary	%temp%MFElogs	Log of migration errors.
EPO450-Checking-Failure.log	Temporary	%temp%MFElogs	List of extensions that have failed to check in.
core-install.log	Install	[InstallDir]\Installer\core	Log file created when the ePolicy Orchestrator installer calls the Orion ANT installer.
epo-install.log	Install	[InstallDir]\Installer\ePO	Log file created when the ePolicy Orchestrator installer calls the Mercury ANT installer.
EpoApSvr.log	Primary	[InstallDir]\DB\Logs	Application Server log file. Present only after initial service startup. Output = RManJNI, DalPolicy, SiteMgr, and SiteMgrWrap.
eventparser.log	Primary	[InstallDir]\DB\Logs	Event Parser log file. Present only after initial service startup. Output = EventParser.
server.log	Primary	[InstallDir]\DB\Logs	ePolicy Orchestrator Server Agent Handler and other C++ code log file. Present only after initial service startup. Output = EPOServer, and Mod_EPO.
errorlog.####-##-##-##_##_##	Apache	[InstallDir]\Apache2\logs	Apache2 log file for the Apache service. Present only after initial service startup.
jakarta_service_########.log	Tomcat	[InstallDir]\Server\logs	Tomcat log file for the Tomcat service. Present only after initial service startup.
localhost_access_log.####-##-##.txt	Tomcat	[InstallDir]\Server\logs	Tomcat log file for the Tomcat service. Present only after initial service startup.
orion.log	Primary	[InstallDir]\Server\logs	Log file used by the McAfee Foundation Services platform and, by default, all loaded extensions. Present only after initial service startup.
stderr.log	Tomcat	[InstallDir]\Server\logs	Tomcat log file for the

Log File Name	Log Type	File Location	Description
			Tomcat service. Present only after initial service startup The file contains any Standard Error output captured by the Tomcat service.

Installing in a Cluster Environment

The ePolicy Orchestrator software provides high availability for server clusters with Microsoft Cluster Server (MSCS) software.

Which operating system are you installing on?

- Windows server 2003
- Windows server 2008

Windows server 2003

Contents

- Requirements
- Setting up the ePolicy Orchestrator cluster
- Testing the ePolicy Orchestrator cluster
- Uninstalling ePolicy Orchestrator

Requirements

Before running ePolicy Orchestrator as a clustered application, ensure that:

- Microsoft Cluster Server (MSCS) is set up and running on a cluster of two or more servers.
- Two separate drives are configured for clustering: a Quorum drive and a Data drive.
- A supported remote database server is configured for the ePO installation:
  - SQL 2005
  - SQL 2008
- The following information is available during installation:
  - The ePolicy Orchestrator virtual server IP address.
  - The ePolicy Orchestrator virtual server name.
  - The ePolicy Orchestrator virtual server FDQN.
  - The location on the Data drive where you intend to place the ePolicy Orchestrator Cluster folder.

CAUTION: The IP address and name of the ePO virtual server should be static and unique. These two identifiers of the ePO virtual server should be listed as resources in the ePolicy Orchestrator group along with the Cluster IP address and Cluster network name that were created when you set up MSCS. To ensure that all four resources appear, avoid using the same identifying information for both the Cluster and the ePO virtual server.

Setting up the ePolicy Orchestrator cluster

Once the requirements are met, use these tasks to set up the nodes of the cluster.

Tasks

- Installing ePolicy Orchestrator on each node
- Creating the ePolicy Orchestrator group
- Creating the data drive
- Creating the IP address resource
- Creating the Network Name resource
- Creating the Generic Service resources

Installing ePolicy Orchestrator on each node

Run the ePolicy Orchestrator Setup on each of the nodes. McAfee strongly recommends that, during installation, only one node at a time be turned on.

Task

1. Double click **Setup.exe** in the installation folder.
2. Follow the wizard until you reach the **Choose Destination Location** page, and specify the path for the shared data drive and click **Next**.

   NOTE: Use this same path for each node.
3. In the **Set Database and Virtual Server Settings**, Select **Enable Microsoft Cluster Server Support**.
4. On the first node only provide the following identifying information for the ePO cluster:
   - The ePO virtual server IP address
   - The ePO virtual server name
   - The ePO virtual server FQDN

   NOTE: This information is automatically provided on subsequent nodes.
5. Complete the installation of ePolicy Orchestrator on the first node as described in *First-Time Installation*.
6. Repeat this task for the second node.

Creating the ePolicy Orchestrator group

Use this task to create an ePO group.

Task

1. Open the Cluster Administrator on the active node:

   Start | All Programs | Administrative Tools | Cluster Administrator
2. Right-click **Groups** in the System Tree, then select **New | Group**. The New Group dialog box appears.
3. Type the **Name** and **Description** of the group, then click **Next**.

4 In the **Preferred Owners** dialog box, identify the owners of the group. Select the desired node under **Available Nodes**, then click **Add**. Repeat until all owners are added, then click **Next**.

5 Click **Finish**.

Creating the data drive

Use this task to create a data drive.

Task

1 In the Cluster Administrator, right-click the **ePO** group, then select **New | Resource**. The New Resource dialog box appears.

2 Type the **Name** and **Description** of the resource, for example, Data Drive.

3 From the Resource type drop-down list, select **Physical Disk**.

4 Ensure that **ePO** is the selected group, then click **Next**.

5 In the Possible Owners dialog box, identify the owners of the resource. Select the desired node, then click **Add**. Repeat until all owners are added, then click **Next**.

6 In the Dependencies dialog box, click **Next**.

7 In the Disk pull-down list, select the disk and click **Finish**.

Creating the IP address resource

Use this task to create the IP address resource.

Task

1 In the Cluster Administrator, right-click the **ePO** group, then select **New | Resource**. The New Resource dialog box appears.

2 Type the **Name** and **Description** of the resource, for example, IP Address.

3 From the Resource type drop-down list, select **IP Address**.

4 Ensure that **ePO** is the selected group, then click **Next**.

5 In the Possible Owners dialog box, identify the owners of the resource. Select the desired node, then click **Add**. Repeat until all owners are added, then click **Next**.

6 No information is required in the Dependencies dialog box. Click **Next**.

7 Type the virtual IP address and subnet mask for the ePO group, then click **Finish**.

Creating the Network Name resource

Use this task to create a Network Name resource.

Task

1 In the Cluster Administrator, right-click the **ePO** group, then select **New | Resource**. The New Resource dialog box appears.

2 Type the **Name** and **Description** of the resource, for example, ePO Server Name.

3 From the **Resource type** drop-down list, select **Network Name**.

4 Ensure that **ePO** is the selected group, then click **Next**.

5 In the Possible Owners dialog box, identify the owners of the resource. Select the desired node, then click **Add**. Repeat until all owners have been added, then click **Next**.

6 In the Dependencies dialog box, select **IP Address**, then click **Next**.

7 Provide the virtual server name for the ePO group, then click **Finish**.

Creating the Generic Service resources

Use this task to create the Generic Service resources.

Task

1 Add Generic Service resources in the following order:

   a McAfee ePolicy Orchestrator 4.5.0 Server

   b McAfee ePolicy Orchestrator 4.5.0 Application Server (Dependency on Server)

   c McAfee ePolicy Orchestrator 4.5.0 Event Parser (Dependency on Application Server)

2 In the Cluster Administrator, right-click the **ePO** group, then select **New | Resource**. The New Resource dialog box appears.

3 Type the **Name** and **Description** of the resource, for example, ePO 4.5 Server.

4 From the **Resource type** drop-down list, select **Generic Service**.

5 Ensure **ePO** is the selected group, then click **Next**.

6 In the Possible Owners dialog box, identify the owners of the resource. Select the desired node, then click **Add**. Repeat until all owners are added, then click **Next**.

7 In the Dependencies dialog box, type the dependency specific to each service.

Service	Dependancy
ePolicy Orchestrator 4.5.0 Application Server	ePolicy Orchestrator 4.5.0 Server
ePolicy Orchestrator 4.5.0 Event Parser	ePolicy Orchestrator 4.5.0 Application Server

8 For each service, type the **Service Name**, leave the **Start Parameters** field blank, then click **Finish**.

Service	Service Name
Server	MCAFEEAPACHESRV
Application Server	MCAFEETOMCATSRV200
Event Parser	MCAFEEEVENTPARSERSRV

Testing the ePolicy Orchestrator cluster

When the ePolicy Orchestrator cluster is set up and online, use this task to ensure that ePolicy Orchestrator functions in a failover situation.

Task

1 Restart the system functioning as the active node. The passive node automatically becomes the active node and you are automatically logged-out.

2 When ePolicy Orchestrator then prompts you to log in, you can conclude that it has continued to function during the failover.

Uninstalling ePolicy Orchestrator

Use this task to remove ePolicy Orchestrator from a system running as a cluster node.

Task

1 Open the Cluster Administrator on the active node:

Start | Program Files | Administrative Tools | Cluster Administrator

2 In the ePolicy Orchestrator Group, right-click each one of the ePO resources, and select **Delete**:

- McAfee ePolicy Orchestrator 4.5.0 Server
- McAfee ePolicy Orchestrator 4.5.0 Application Server
- McAfee ePolicy Orchestrator 4.5.0 Event Parser

3 Open the Windows Control Panel, select **Add or Remove Programs**, select **McAfee ePolicy Orchestrator**, then click **Change/Remove**.

Windows server 2008

Contents

- Requirements
- Setting up the ePolicy Orchestrator cluster
- Testing the ePolicy Orchestrator cluster
- Uninstalling ePolicy Orchestrator

Requirements

Before running ePolicy Orchestrator as a clustered application, ensure that:

- Microsoft Failover Clustering is set up and running on a cluster of two or more servers.
- Two separate drives are configured for clustering:
  - A Quorum drive
  - A Data drive
- A supported remote database server is configured for the ePO installation:
  - SQL 2005
  - SQL 2008
- The following information is available during installation:
  - The ePolicy Orchestrator virtual server IP Address
  - The ePolicy Orchestrator virtual server name
  - The ePolicy Orchestrator virtual server FQDN
  - The location on the data drive where you intend to place the ePolicy Orchestrator cluster folder

CAUTION: The IP address and name of the ePO virtual server should be static and unique. These two identifiers of the ePO virtual server should be listed as resources in the ePolicy

Orchestrator group along with the Cluster IP address and Cluster network name that were created when you set up MSCS. To ensure that all four resources appear, avoid using the same identifying information for both the Cluster and the ePO virtual server.

Setting up the ePolicy Orchestrator cluster

Once the requirements are met, use these tasks to set up the nodes of the cluster.

Before you begin

Before configuring and installing ePolicy Orchestrator 4.5, run the "Validate a Configuration" tool in "Failover Cluster Management" to ensure your cluster configurations is setup correctly.

Tasks

- Installing ePolicy Orchestrator on each node
- Creating the ePolicy Orchestrator application group
- Creating the Client Access Point
- Creating the data drive
- Creating the Generic Services resources

Installing ePolicy Orchestrator on each node

Run the ePolicy Orchestrator setup on each of the nodes.

Task

For option definitions, click **?** in the interface.

1. Double click **Setup.exe** in the installation folder.
2. Follow the wizard until you reach the **Choose Destination Location** page, and specify the path for the shared data drive and click **Next**.

   NOTE: Use this same path for each node.

3. In the **Set Database and Virtual Server Settings**, Select **Enable Microsoft Cluster Server Support**.
4. On the first node only provide the following identifying information for the ePO cluster:
   - The ePO virtual server IP address
   - The ePO virtual server name
   - The ePO virtual server FQDN

   NOTE: This information is automatically provided on subsequent nodes.

5. Complete the installation of ePolicy Orchestrator on the first node as described in *First-Time Installation*.
6. Repeat this task for the second node.

Creating the ePolicy Orchestrator application group

Use this task to create the ePolicy Orchestrator application group.

Task

For option definitions, click **?** in the interface.

1. Open the Failover Cluster Management tool on the Active Node by clicking **Start | Programs | Administrative Tools | Failover Cluster Management**.
2. 1) Right-click **Services and Applications** in the cluster management tree, then select **More Actions... | Create Empty Service or Application**.
3. Right-click **New service or application** and select **Rename** to name the Application Group to "ePO".

Creating the Client Access Point

Use this task to create the client access point.

Task

For option definitions, click **?** in the interface.

1. Right-click on the **ePO** Application Group and select **Add a resource | Client Access Point.** The **Client Access Point Wizard** appears.
2. Type the ePO Virtual Name in the **Name** field and specify the Virtual IP in the **Address** field, then click **Next**. The **Confirmation** page displays.
3. Click **Next** to allow the Client Access Point to be configured. Click **Finish** when the Wizard is complete.
4. If the Client Access Point is offline, right-click on the name and choose **Bring this resource online**.

Creating the data drive

Use this task to create the data drive.

Task

For option definitions, click **?** in the interface.

1. Right-click the **ePO** Application Group and select **Add Storage.** The **Add Storage** dialog displays.
2. Select the data drive to be used for your ePolicy Orchestrator installation and click **OK**.

Creating the Generic Services resources

Use these tasks to create the Generic Services resources needed for use with ePolicy Orchestrator in a cluster environment.

Tasks

- Creating the server resource
- Creating the Application Server resource
- Creating the Event Parser resource

Creating the server resource

Use this task to create the McAfee ePolicy Orchestrator 4.5.0 server resource.

Task

For option definitions, click **?** in the interface.

1. Right-click the **ePO** Application Group and select **Add a resource | Generic Service.** The Select Service Wizard appears.
2. Select **McAfee ePolicy Orchestrator 4.5.0 Server** and click **Next**. The Confirmation page displays.
3. Click **Next** to allow the Generic Service to be created. Click **Finish** when the Wizard is complete.
4. Right-click the **McAfee ePolicy Orchestrator 4.5.0 Server** resource and choose **Properties.** The Properties dialog appears.
5. On the General tab, remove the **Startup parameters** and add a blank space.

   NOTE: Apache will not start with any startup parameters specified and an empty entry is not permitted, so that is why a blank space is needed.

Creating the Application Server resource

Use this task to create the McAfee ePolicy Orchestrator 4.5.0 Apoplication Server resource.

Task

For option definitions, click **?** in the interface.

1. Right-click the **ePO Application Group** and select **Add a resource | Generic Service.** The Select Service Wizard appears.
2. Select **McAfee ePolicy Orchestrator 4.5.0 Application Server** and click **Next**. The Confirmation page displays.
3. Click **Next** to allow the Generic Service to be created. Click **Finish** when the Wizard is complete.
4. Right-click the **McAfee ePolicy Orchestrator 4.5.0 Application Server** resource and select **Properties**. The Properties dialog appears.
5. Click the **Dependencies** tab and then add **McAfee ePolicy Orchestrator 4.5.0 Server** as a dependency.

Creating the Event Parser resource

Use this task to create the McAfee ePolicy Orchestrator Event Parser resource.

Task

For option definitions, click **?** in the interface.

1. Right-click the **ePO Application Group** and select **Add a resource | Generic Service**. The Select Service Wizard appears.
2. Select **McAfee ePolicy Orchestrator 4.5.0 Event Parser** and click **Next**. The Confirmation page displays.

3 Click **Next** to allow the Generic Service to be created. Click **Finish** when the Wizard is complete.

4 Right-click the **McAfee ePolicy Orchestrator 4.5.0 Event Parser** resource and select **Properties**. The Properties dialog appears.

5 Click the **Dependencies** tab and then add **McAfee ePolicy Orchestrator 4.5.0 Application Server** as a dependency.

Testing the ePolicy Orchestrator cluster

When the ePolicy Orchestrator cluster is set up and online, use this task to ensure that ePolicy Orchestrator functions in a failover situation.

Task

For option definitions, click **?** in the interface.

1 Restart the system functioning as the active node. The passive node automatically becomes the active node and you are automatically logged-out.

2 When ePolicy Orchestrator prompts you to log in, you can conclude that it has continued to function during the failover.

Uninstalling ePolicy Orchestrator

Use this task to remove ePolicy Orchestrator from a system running as a cluster node.

Task

For option definitions, click **?** in the interface.

1 To open the Failover Cluster Management tool on the Active Node, click **Start | Programs | Administrative Tools | Failover Cluster Management**.

2 In the ePO application group, right-click each one of the following ePO resources, and select Delete:

- McAfee ePolicy Orchestrator 4.5.0 Server
- McAfee ePolicy Orchestrator 4.5.0 Application Server
- McAfee ePolicy Orchestrator 4.5.0 Event Parser

3 Open the Windows Control Panel and select **Programs and Features**, then select **McAfee ePolicy Orchestrator** and click **Uninstall/Change**. Repeat this step for every node.